Electronic Signatures for Medical Records

RSA 2002 Conference

Ann Geyer
Tunitas Group
209-754-9130
ageyer@tunitas.com
www.tunitas.com
PKI Applied to Healthcare

- **Traditional PKI positioning does not work well in healthcare**
  - The promise to improve security at lower cost while enabling new applications is ineffective
  - Healthcare wants PKI to be a built-in component of critical healthcare business processes and applications

- **PKI must be seen as solution to ‘big’ problem**
  - Kaiser’s PKI success due in part because it secures Kaiser’s most sensitive and critical clinical applications

- **Electronic signature of medical records is a Big Picture Problem that PKI can address**
Objectives

- Describe why medical record signature is important
- Identify signature properties required to satisfy signatures for electronic medical record (EMR) uses
- Discuss emerging trends for healthcare electronic signature
- Critique current industry esignature practices
- Present healthcare efforts to standardize esignatures on medical records
- Identify business and regulatory risks related to healthcare esignature efforts
An Industry in Crisis

- **Preventable medical error**
  - Institute of Medicine ~ 100k deaths annually attributable to error
  - Errors correlated with failure to communicate, workflow disruptions

- **Managed care failure to contain medical cost**
  - Managed Care Indicted -- treatment options reduced, cost of care increased during zero inflation period
  - National CMS study shows costs increased 7% in 2000

- **Provider insolvency restricts access to medical innovations**
  - Non-profit industry, with poor bond ratings, dependent upon fundraising to offset operational losses
  - Poor candidate for at-risk capital investments
Many Culprits

- Inefficient reimbursement
- Below cost contracting
- Restrictive regulation
- Uninsured population
- Poor business management

... 

- Overwhelming reliance upon paper records, oral communication and human memory
Handwritten Orders

- **Plendil**
  For: heart pain/value problems
  Dosage: 80 milligrams

- **Isodril**
  For: high blood pressure
  Dosage: 10 milligrams
And the Patient Died!

- **Landmark wrongful death case in Texas**
- **Cardiologist, Pharmacist and Pharmacy all judged jointly liable for wrongful death**
  - $450k judgement
  - ‘technology available to practitioners that could have avoided erroneous dispensing’
Medical Record Isolation

- **Medical knowledge increases faster than practitioners can absorb**
  - Number of new drugs doubles annually
  - New specialty based medical articles average >1000 annually
  - New surgical procedures and medical treatments overwhelm any provider

- **Paper records inhibit data analysis and linking**
  - Alerts
  - New interpretations
  - Compliance to treatment protocols
  - Potential drug interactions

- **EMR required to leverage evidence-based medicine**
**Inefficient Reimbursement**

- **Reimbursement depends upon medical records**
  - More than half of healthcare claims require review of information from the medical record prior to payment
  - Medical necessity determinations, compliance with non-aggressive treatment protocols

- **Duplicating and shipping paper medical records is costly and time-consuming**
  - Billing costs frequently exceed reimbursement level for simple procedures
  - Lost records push accounts payable timeframes to months and years
HIPAA Administrative Simplification

- **Claims attachment (ANSI X12.278)**
  - Transaction for requesting and providing additional medical record information to adjudicate a claim
  - Administrative ROI depends upon an effective electronic claim attachment
  - Electronic claims attachments are hindered by paper records
Electronic Medical Records

Historically
- Expensive and difficult to cost justify
- Proprietary products requiring 1-1 interfaces to all clinical and billing feeder systems
- Require providers to change their behavior

Emerging Trend
- Corporate and organized medicine have new liability forcing the use of electronic medical records
- State laws now require hospitals implement “computerized physician order entry” systems
- LeapFrog Group members (large healthcare purchasers) are including CPOE requirements in plan contracts
Electronic Medical Records

- **Emerging Trends (cont’d)**
  - EMR permits automated treatment review with decision support applications to identify effective or potentially harmful treatment methods
  - Recent EMR initiatives have positive ROI and payback on the order of 3 years by improving reimbursement documentation

- **But ...**
There is No Record without a Signature

- Medicare requires all entries in a medical record be authenticated with a signature
  - Medical practice requires practitioner signature to note responsibility for clinical order / record
  - “It’s not a medical record without signature”

- Specific state laws require practitioner signature on
  - Pharmacy prescriptions
  - Clinical orders
  - Selected transcribed reports
  - Various hospital intake, discharge & charting forms

- Plans have varying requirements for signature on medical or administrative records used to process claims
What Electronic Signature for EMR?

- **Not just any electronic signature, but one that works for electronic medical records**

- **Properties derived from medical record purposes determine acceptable solutions**
  - Regulatory compliance
  - Liability defense
  - Reimbursement
Regulatory Compliance

- **Rules typically apply to institutions, licensed practitioners, pharmacies, and pharmacists**

- **Where allowed, esignature of medical record must be timely and unique to signatory**
  - Over 35 states with healthcare signature laws
  - JCAHO Information Management Standards

- **Loosely stated requirements**
  - Attestation of ownership and exclusive use of practitioner’s ‘computer code’
  - Internal security controls left to implementers
**Liability Defense**

- **Medical record is central to practitioner and institutional liability (malpractice) defense**
  - Signature authenticity is central to admissibility
  - But record authenticity is more frequently challenged

- **Federal E-SIGN Legislation**
  - Set standards for resolving signature disputes, through endorsement of UETA
  - Dispute resolution requires “…examination of the efficacy of the security procedures used to authenticate the signer”
  - Parties agree on acceptable controls
  - Provided controls are properly implemented, assume risk of failure
Liability Defense (cont’d)

- **Third party interest**
  - E-SIGN gives privity to parties engaging in the transaction, but does not negate 3rd party interest in the transaction integrity
    - Many healthcare transactions between providers or provider-plan also have a third party interest
    - Third parties can be patients, payers, regulators, state agencies
  - Third party may challenge the adequacy of controls agreed to by the transactions principals
Liability Defense (cont’d)

- **Need strong form of ‘non-repudiation’**
  - Non-repudiation without presumption about the adequacy of controls

- **Requires long term persistence of signature**
  - Legal interest in record occurs subsequent to discovery of injury from alleged malpractice
  - Medical record retention requirements range from 7-18 years for most liability purposes
  - Signatures must retain their ability to be authenticated over this timeframe
Reimbursement

- Under HIPAA, medical record signature must be transportable as part of EDI message
  - Multiple message envelops … HL7 inside X12.275
  - Claim attachment standard developing slowly

- Third party payer requires signature verification
  - At the time of signature, it’s generally unknown what third party(s) may need to verify the signature
  - Consequently, medical record esignatures must be independently verifiable
Electronic Signature Properties for Medical Records

- **From Regulation**
  - Unique with ownership and control agreements

- **From Liability Defense**
  - Non-repudiation in legal disputes

- **From Reimbursement**
  - Transportability
  - Independent verifiability
Current Practice

- **Re-authentication using shared secret**
  - Asked to re-enter pin at various points in application to indicate authorship, agreement, approval, etc.
  - Designed to satisfy regulatory requirements
  - There is no explicit signature representation
  - Applications will render stored image of practitioners signature

- **Record authenticity depends on:**
  - Software engineering controls
  - Configuration management
  - Integrity of the audit logs for configuration and record events
  - Personnel supervision
  - ‘Total System Security’
Current Practice Fails

- **Non-repudiation**
  - Means asserting the business rules were appropriately and consistently applied
  - Equivalent to proving there has been no breach of internal controls for the entire period from signature to dispute

- **Persistence**
  - Signature is implicit in the application of business rules
  - Version and system changes challenge persistence

- **Independent verifiability & transportability**
  - Signature acceptance relies entirely on trust given to the record owner
Digital Signature

- **HIPAA included an electronic signature mandate**
  - 1998 HIPAA Security NPRM included proposal for a digital signature standard but since withdrawn for more study
  - Applied only to administrative transactions … today only some medical record attachments might have signature but HIPAA requirement will be presumptive for other applications

- **Significant legislative & regulatory activity surrounding electronic prescription**
  - DEA rules will soon allow electronic prescription of narcotics with proper digital signature (NPRM promised Q1, 2002)
  - State laws (e.g. California AB1589) for digital signature on ePrescription of all drugs

- **ANSI Health Informatics Standards Board**
  - Evaluating options for recommending digital signature as standard
EMR Signature Representation

- An appropriate representation and coding scheme will
  - Support additional EMR signature events
    - Multiple signatures
    - Counter-signatures
    - Signature sequencing
  - Communicate the intent of the signatory
    - Signature type and the signer’s healthcare role(s)
**Signature Purpose**

- **EMR signature types distinguished by signers’ role or function**
  - Authorship and co-authorship
  - **Co-participant** -- participant in the underlying event; surgeon signing an operative report
  - **Transcriptionist** or recorder
  - **Verification** -- physician counter-signing previously recorded verbal order
  - **Validation** -- to support inclusion into record of document created by less privileged staff such as a medical student or resident
  - **Witness** (multiple types)
  - **Addendum / Modification / Administrative** -- signature types to indicate changes to previous documents
Signature Purpose (cont’d)

- **EMR signature types to represent actions of automated processes**
  - **Source Signature**
    - Device signatures such as ECG systems, biomedical monitors, imaging systems, lab systems
  - Review Signature
    - Quality control review, record completeness
  - Timestamp
    - Medical record events
    - Signatures
Healthcare Standards

- **ASTM 31.20 Committee on Health Informatics**
  - **E1762** -- defines general esignature requirements and attributes being updated to align with E-Sign and to incorporate xml-dsig representation
  - **E2084** -- provides ASN.1 modules for representing healthcare signature and signer attributes within PKCS#7 structure

- **HL7 -- clinical messaging format**
  - **CCOW** -- new standard to manage clinical context.
  - **Will include specifications for a common digital signature capability**
  - **Allows for single signature application across clinical systems**
Outlook

- **No waiting for completed PKI infrastructure**
  - Attestation and Direct Trust Models move digital signatures along
  - Existing precedence for reliance upon practitioner’s attestation is used to validate public key ownership / simplify interoperability
  - Signed transactions are between ‘contracted’ parties which makes direct trust feasible

- **Substantial opportunity for process improvement and cost savings**
  - Typically 2FTE per facility dedicated solely to signature collection
  - Paper management & retention costs

- **General recognition that esignature is an important component of ehealth initiatives**
Potholes

- **HHS must clarify HIPAA regulation and Medicare rules**
  - CMS failed to rewrite its signature rules to permit electronic documents and signatures as required by US E-Sign
  - CMS historically late to understand and incorporate technology solutions
    - As late as 1998, CMS banned use of Internet for any communication of Medicare patient info due to ‘unavailability of adequate encryption technology’
  - HHS generally does not participate in healthcare standards activities and only recently a joined the FedPKI workgroup

- **States also regulate medical records**
  - Few have rewritten medical record signature laws
Potholes

- **Digital Signatures may add too much accountability**
  - A strong esignature model may necessitate change in medical practice workflow
  - Current handwritten signature practices allow for signature stamps tacitly exercised by practitioner delegate

- **Integration difficulties**
  - Most medical records created and maintained within proprietary stovepipe systems
  - Mature product market where vendors will add capability only in response to unambiguous market requirements

- **Industry Inertia -- Expedient Solutions**
  - Digital signatures not yet an accepted industry solution, early adopters are still needed to prove utility
Final Comments

- **Healthcare moves slowly unless**
  - Regulation, Reimbursement or Liability concerns are clear

- **Electronic signatures are necessary to address**
  - Regulation, Reimbursement and Liability issues

- **Current esignatures exist only inside EMR applications**
  - Have limited benefits for transactions requiring healthcare signature properties

- **Digital signatures provide all necessary signature properties and attributes in a standard way**